



SPYWOLF

Security Audit Report



Completed on
February 5, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **AI Wallet** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”



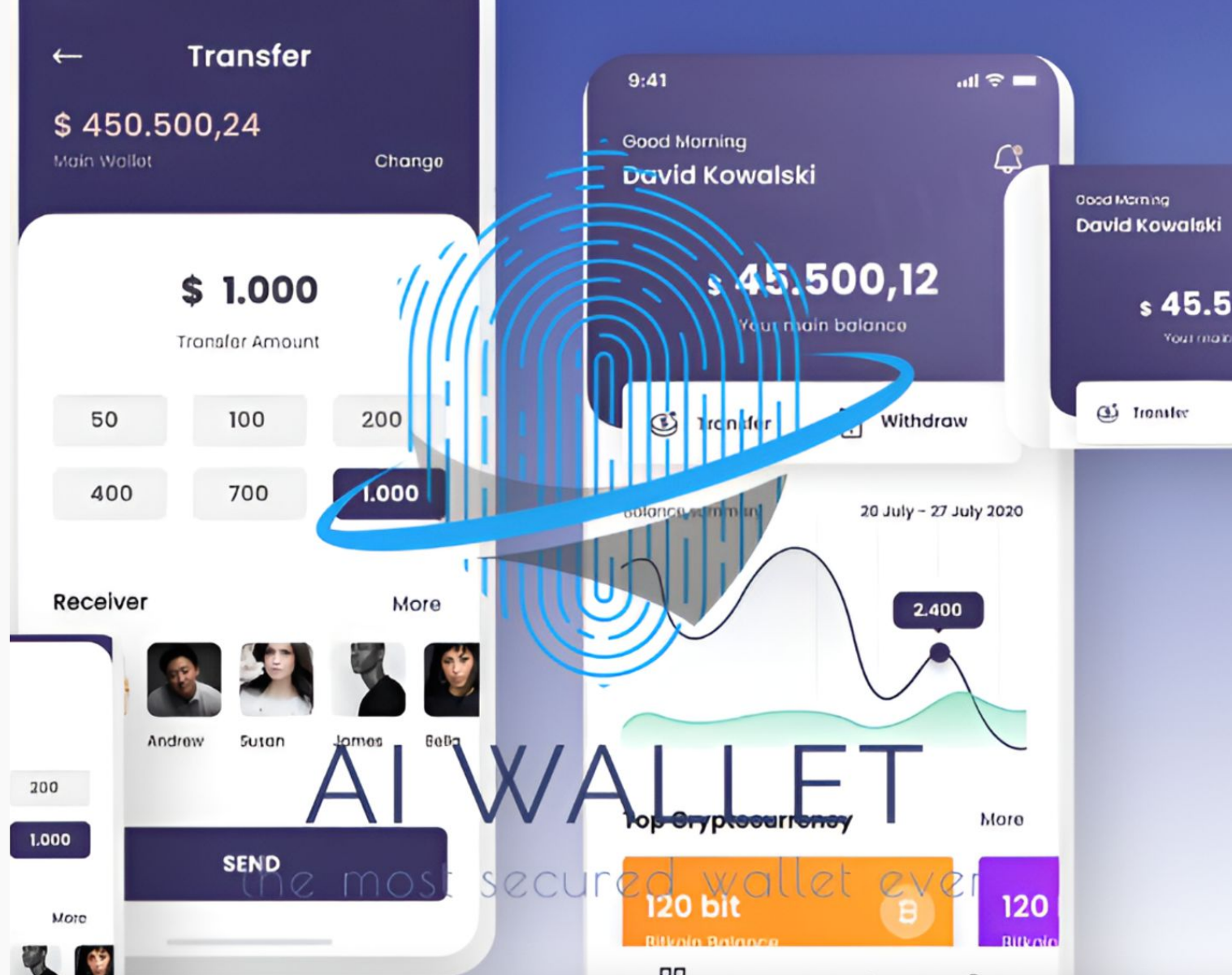


TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03
Featured Wallets	04
Vulnerability Check	05
Threat Levels	06
Found Threats	07-A/07-B
Good Practices	08
Tokenomics	09
Team Information	01
Website Analysis	12
Social Media & Online Presence	12
About SPYWOLF	13
Disclaimer	14



AI WALLET



PROJECT DESCRIPTION

According to their website/whitepaper:

"You can place buy and sell orders for a token at the prices you set without using swaps. When AI Wallet comes to the price you want, it automatically buys it for you using the most accurate tax in our SWAP system. The transaction will never be canceled and you will not pay a fee for nothing. The tokens you receive will automatically appear in your AI Wallet"

Release Date: Launched February 3

Category: Wallet



CONTRACT INFO

Token Name

AI Wallet

Symbol

AIW

Contract Address

0x332C7B139f4dCb70B5154163a99C4EDFAfcee6a0

Network

Ethereum

Language

Solidity

Deployment Date

Feb 05, 2023

Verified?

Yes

Total Supply

1,000,000 AIW

Status

Not Launched

TAXES

Buy Tax

5%

Sell Tax

5%

*Taxes cannot be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



TOKEN TRANSFERS STATS

Transfer Count	1058
Uniq Senders	240
Uniq Receivers	380
Total Amount	84137070.91714898 AIW
Median Transfer Amount	44948.041280169 AIW
Average Transfer Amount	79524.64169862852 AIW
First transfer date	2023-02-04
Last transfer date	2023-02-05
Days token transferred	1

SMART CONTRACT STATS

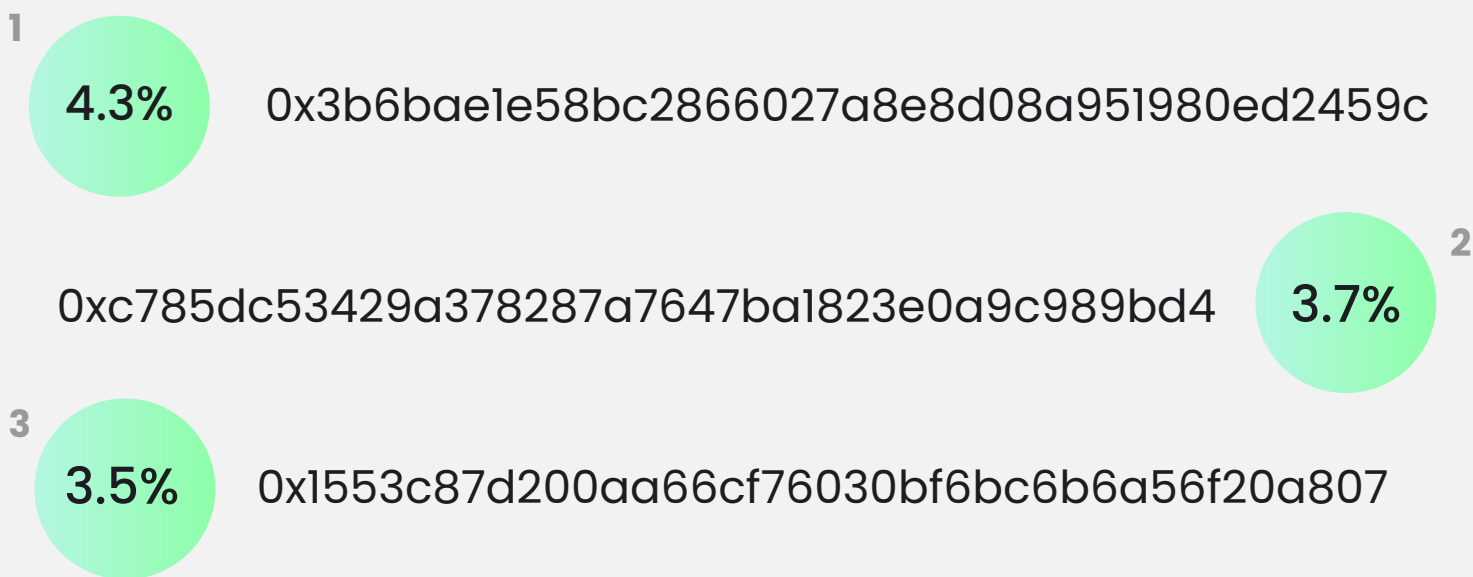
Calls Count	3606
External calls	322
Internal calls	3284
Transactions count	1314
Uniq Callers	340
Days contract called	1
Last transaction time	2022-12-25 10:37:35 UTC
Created	2022-12-25 01:36:47 UTC
Create TX	0xf4447c13a70ab362b000e9237dff12045a6c87a7cd5b662cd2c2c573bf47e317
Creator	0xb94ff0b04c4c53f10da2017b1612910bfee74a1l



FEATURED WALLETS

Owner address	0x00 Ownership is renounced <i>Original owner: 0xb94ff0b04c4c53f10da2017b1612910bfee74a11</i>
Marketing wallet	0x93174d290E3A2479071B5Feb5b64cA3bD963f553
Development wallet	0xb94ff0b04c4c53f10da2017b1612910bfee74a11
LP address	Uniswap: 0xe74d8b67fbcbbcacfa66cfaa6fa7f8b7970e11a5

TOP 3 UNLOCKED WALLETS





VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ High Risk

Development wallet and marketing wallet can initiate manual token swaps from contract and withdraw eth from the contract. If contract's token swap balance is 0 transactions will fail.

```
function manualswap() external {
    require(_msgSender() == _developmentAddress || _msgSender() == _marketingAddress);
    uint256 contractBalance = balanceOf(address(this));
    swapTokensForEth(contractBalance);
}

function manualsend() external {
    require(_msgSender() == _developmentAddress || _msgSender() == _marketingAddress);
    uint256 contractETHBalance = address(this).balance;
    sendETHToFee(contractETHBalance);
}
```

**Contract's ownership is renounced.
Owner does not have any special privileges.**



Informational

Before ownership renouncement owner could:

Enable/disable trading, blacklist address from trading.

Set fees without limit, set max transaction amount without limit.

```
function setTrading(bool _tradingOpen) public onlyOwner {
    tradingOpen = _tradingOpen;
}

function blockBots(address[] memory bots_) public onlyOwner {
    for (uint256 i = 0; i < bots_.length; i++) {
        bots[bots_[i]] = true;
    }
}

function setFee(uint256 redisFeeOnBuy, uint256 redisFeeOnSell,
uint256 taxFeeOnBuy, uint256 taxFeeOnSell) public onlyOwner {
    _redisFeeOnBuy = redisFeeOnBuy;
    _redisFeeOnSell = redisFeeOnSell;

    _taxFeeOnBuy = taxFeeOnBuy;
    _taxFeeOnSell = taxFeeOnSell;
}

function setMaxTxnAmount(uint256 maxTxAmount) public onlyOwner {
    _maxTxAmount = maxTxAmount;
}
```

**Contract's ownership is renounced.
Owner does not have any special privileges.**



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

AI WALLET

GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot stop or pause the contract
- ✓ The owner can set a transaction limit, but can't lower it than 1% of total supply
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



There is no information about the initial token distribution in their website and/or whitepaper.

TOKENOMICS



THE TEAM

! The team is anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://aiwalleterc.com/>

Domain Registry

<https://www.hostinger.com>

Domain Expiration

Expires on 2024-02-03

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Very nice color scheme and overall layout.

Content

The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper

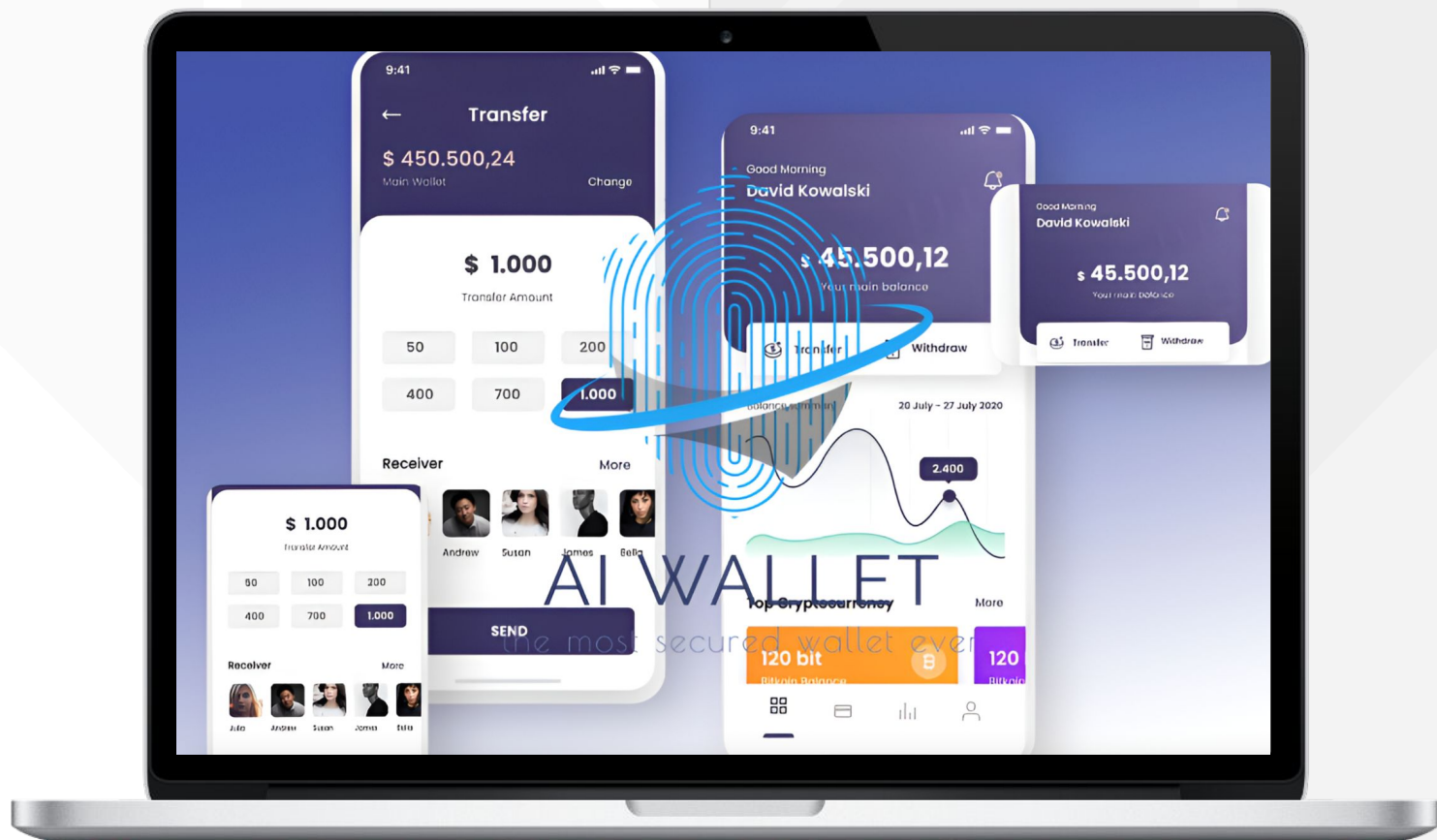
No whitepaper found

Roadmap

Yes

Mobile-friendly?

Yes



aiwalleterc.com

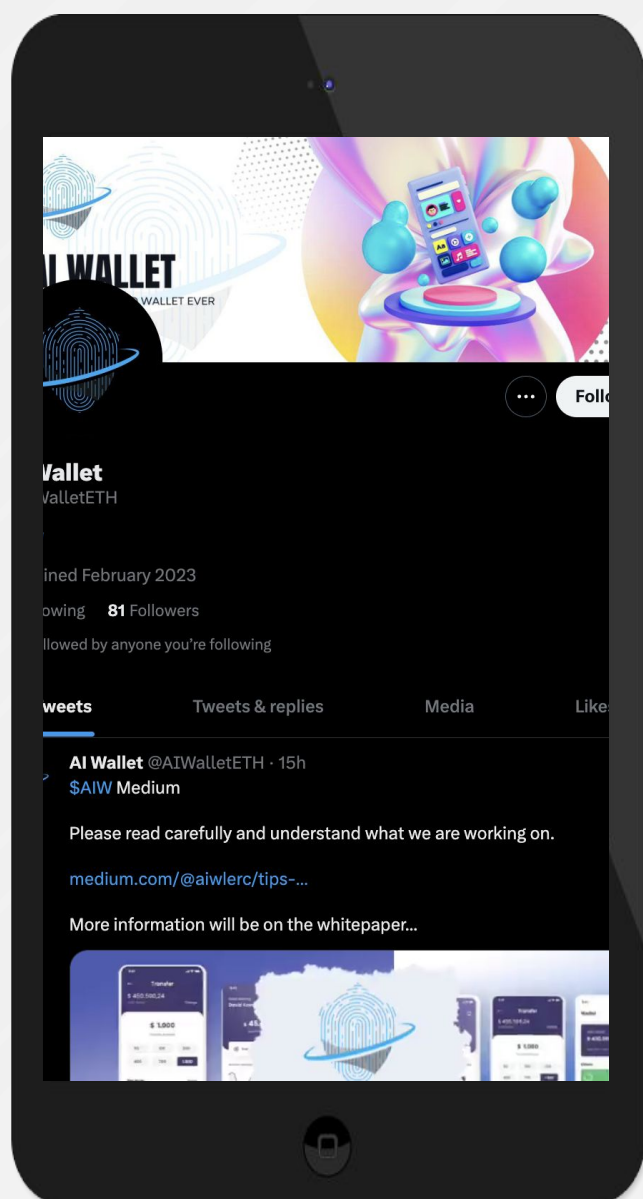


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

Project's social media activity is concentrated in telegram with organic users interactions.



Twitter

@AIWalletETH

- 81 followers
- Daily posts



Discord

- Not available



Telegram

@aiwalleteth

- 112 members
- Active community and mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.